S.D. INDEVAL
Instituto para el Depósito de Valores

Firmas Digitales

Manual de Usuario

Versión 1.1

© 2006 S.D. Indeval. Este documento fue elaborado por Bursatec para Indeval.

Toda la información aquí contenida es propiedad de la institución y debe considerarse como confidencial en los términos definidos por el área Jurídica del Indeval. Queda estrictamente prohibida la reproducción parcial o total de este documento a cualquier persona.

Contenido general

Introducción **5**

Objetivo 5

Audiencia 5

Antecedentes 5

Descripción general del sistema 5

Estructura 6

Glosario **7**

Prerrequisitos **9**

Navegador de Internet 9

Máquina Virtual de Java 9

Uso de Applets habilitado 9

Certificado digital en formato PKCS12 (PFX) 9

Firma Digital **10**

Pasos para el firmado de operaciones 10

Captura de Instrucciones 10

Firma digital de instrucciones 12

Errores en la Firma Digital 14

Anexos **16**

Validación de versión del navegador de internet 16

Validación de JVM 18

Instalación de JVM 18

Generación de Certificados PKCS12 22

5.1.4.2 Pasos para generar el Certificado PKCS12 22

Instrucciones 22

1. Ejecutar la aplicación InstaladorCertificados.exe 22

2. Datos de Captura 23

Recomendaciones **28**

Respaldo de Certificado Digital y Llave Privada 28

Generación de Certificados PFX 28

Rutas de almacenamiento para los certificados 28

Contraseñas de certificados ..... **¡Error! Marcador no definido.**
Uso de contraseñas seguras para los certificados PFX 28
Certificados Digitales 30
Referencias 33

Introducción

Objetivo

El objetivo de este documento es explicar el uso del firmado digital para las instrucciones capturadas en el Portal INDEVAL.

Audiencia

Este documento está orientado a los usuarios finales (Participantes) del Portal INDEVAL.

Antecedentes

El INDEVAL recibe mensajes por parte de los Participantes para la realización de actividades como solicitud o modificación a la posición en títulos o saldo en efectivo de las cuentas. Estos mensajes, conocidos como instrucciones, son recibidos por INDEVAL a través del Módulo de Comunicaciones del Nuevo Sistema INDEVAL usando un formato de mensajes basado en el estándar ISO 15022, o bien, a través de una aplicación Web conocida como Portal INDEVAL.

1. El uso de firmas digitales se implementó con el objetivo de aumentar el nivel de seguridad de las transacciones que se realizan en el Portal INDEVAL. El uso de las firmas digitales permitirá asegurar la integridad, autenticidad y no repudiación (es decir, la no negación) de las instrucciones enviadas por este medio.

Los participantes podrán enviar las instrucciones de dos maneras:

- Instrucciones capturadas individualmente en una pantalla de captura del Portal INDEVAL y firmadas digitalmente en el navegador del participante.

- Instrucciones en un archivo por lotes cargadas por medio de una forma de File Transfer del Portal INDEVAL y firmadas digitalmente en el navegador del participante.

Para poder firmar digitalmente las instrucciones en el Portal INDEVAL, cada Participante requerirá un certificado digital con formato PFX. El participante podrá utilizar la aplicación de escritorio llamada **Asistente para Instalación de Certificado PFX** (InstaladorCertificados.exe) para obtener el certificado digital en formato PFX.

Descripción general del sistema

Para firmar digitalmente las instrucciones enviadas al INDEVAL por medio del Portal, se utilizan las siguientes herramientas:

1. El Asistente para Instalación de Certificado PFX (InstaladorCertificados.exe), que es una aplicación de escritorio que permite generar el certificado digital PFX con que se firmarán las instrucciones.

2. Una página en el Portal INDEVAL que realiza la firma de las instrucciones.

El uso del sistema de firmas digitales tiene los siguientes requisitos:

1. Navegador Internet Explorer versión 6.0 o superior, o el navegador Firefox versión 1.6 o superior.

2. Máquina Virtual de Java versión 1.5 o superior.

3. Habilitado en su navegador de internet la opción de uso de Applets.

Los usuarios que cumplan estos requisitos, podrán realizar el firmado digital por medio de un Applet. Ver la sección Anexos para aprender cómo verificar si cumple con los requisitos, y qué hacer para cumplir con ellos si le falta alguno.

Estructura

Las secciones de este documento se describen a continuación.

Capítulo 1. Introducción. Introduce al Participante al sistema y al resto de este Manual de Usuario.

Capítulo 2. Glosario. Describe los conceptos nuevos que se utilizan en este documento.

Capítulo 3. Prerrequisitos. Describe los prerrequisitos para utilizar el sistema de firmas digitales y los pasos necesarios para cumplirlos.

Capítulo 4. Firma Digital. Describe los pasos para realizar la firma digital de Instrucciones.

Capitulo 5.- Anexos. Describe la forma de realizar tareas adicionales para la configuración y uso de las firmas digitales.

Capítulo 6. Recomendaciones. Describe una serie de recomendaciones que se deben tomar en cuenta para hacer uso del modulo de Firmas Digitales.

Capítulo 7. Referencias. Incluye ligas a sitios de interés o utilidad para que el Participante cumpla con los requisitos para utilizar el sistema de Firmas Digitales

Glosario

Autoridad de certificación. Autoridad de certificación o autoridad certificante (AC) es una entidad que emite certificados digitales para su uso por terceros.

Applet. Es un componente de una aplicación que se ejecuta en el contexto de otro programa, por ejemplo un navegador web.

CER. Un archivo con extensión CER es un archivo que almacena un certificado digital codificado que cumple el estándar UIT-T X.509.

Certificado de Autoridad. En criptografía una Autoridad de certificación, certificadora o certificante (AC o CA por sus siglas en inglés Certification Authority) es una entidad de confianza, responsable de emitir y revocar los certificados digitales o certificados, utilizados en la firma electrónica, para lo cual se emplea la criptografía de clave pública. El Certificado de Autoridad es el certificado digital de la Autoridad de Certificación.

Certificado Digital. Un Certificado Digital es un documento digital mediante el cual un tercero confiable (una autoridad de certificación) garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública.

Contraseña Maestra. Una Contraseña Maestra es una contraseña que se utiliza en Firefox para proteger información sensible tal como la contraseña de sitios web o de un certificado digital.

Criptografía. La criptografía es la ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos.

CVE. Un archivo con extensión CVE es un archivo que almacena una llave privada.

Firefox (Mozilla Firefox). Mozilla Firefox es un navegador de Internet, con interfaz gráfica de usuario desarrollado por la Corporación Mozilla y un gran número de voluntarios externos.

Firma digital. La firma digital es un método criptográfico que asocia la identidad de una persona o de un equipo informático al mensaje o documento. En función del tipo de firma, puede, además, asegurar la integridad del documento o mensaje. La firma electrónica, como la manuscrita, puede vincularse a un documento para identificar al autor, para señalar conformidad (o disconformidad) con el contenido, para indicar que se ha leído o, según el tipo de firma, garantizar que no se pueda modificar su contenido.

Internet Explorer (Microsoft Windows Internet Explorer). Microsoft Windows Internet Explorer (también conocido antes como Internet Explorer, IE o MSIE) es un navegador de Internet producido por Microsoft para su plataforma Windows. Actualmente es el navegador de Internet más popular y más utilizado en el mundo. Es el navegador que se instala automáticamente con el sistema operativo Windows.

ISO 15022. ISO 15022 es un estándar para mensajes de títulos valor. Este estándar fue desarrollado por la industria de valores y contiene un conjunto de reglas y guías para construir mensajes. Si se siguen estas reglas y guías, el mensaje resultante (formato) cumple automáticamente con el estándar ISO 15022. Algunos ejemplos son MT 540 y MT 548.

Llave privada. La criptografía asimétrica es un método criptográfico que usa un par de llaves para el envío de mensajes. Las dos llaves pertenecen a la misma persona a la que se ha enviado el mensaje. Una llave es pública y se puede entregar a cualquier persona. La otra llave es privada y el

propietario debe guardarla de modo que nadie tenga acceso a ella. El remitente usa la llave pública del destinatario para cifrar el mensaje, y una vez cifrado, sólo la llave privada del destinatario podrá descifrar este mensaje.

Máquina Virtual de Java. La máquina virtual de Java (en inglés Java Virtual Machine, JVM) es un programa nativo, es decir, ejecutable en una plataforma específica, capaz de interpretar y ejecutar instrucciones expresadas en un código binario especial (el Java bytecode), el cual es generado por el compilador del lenguaje Java.

.NET FRamework. Es un componente de software que puede ser añadido al sistema operativo Windows. Provee un extenso conjunto de soluciones predefinidas para necesidades generales de la programación de aplicaciones, y administra la ejecución de los programas escritos específicamente con la plataforma. Esta solución es el producto principal en la oferta de Microsoft, y pretende ser utilizada por la mayoría de las aplicaciones creadas para la plataforma Windows.

PFX. PFX (Personal Information Exchange) es un estándar utilizado para intercambiar objetos públicos y privados en un solo archivo. Fue reemplazado por el estándar PKCS #12.

PKCS #12. Es un estándar PKCS (Public Key Cryptography Standards) que define un formato de archivo usado comúnmente para almacenar llaves privadas con su certificado de llave pública protegido mediante llave simétrica. Es un estándar que siguió a PFX, y que se manejan como equivalentes en este documento.

Plug-in. Un plugin (o plug-in, también conocido como addin, add-in, addon o add-on) es una aplicación informática que interactúa con otra aplicación para aportarle una función o utilidad específica, generalmente muy específica, como por ejemplo servir como driver (controlador) en una aplicación, para hacer así funcionar un dispositivo en otro programa. Esta aplicación adicional es ejecutada por la aplicación principal.

Prerrequisitos

Esta sección del documento describe los prerrequisitos para poder utilizar el sistema de firmas digitales.

Navegador de Internet

Cualquiera de los siguientes navegadores:

- Microsoft Windows Internet Explorer versión 6.0 o superior.
- Mozilla Firefox versión 1.6 o superior.

Nota: Para saber la versión del navegador ver Anexo.

Máquina Virtual de Java

- Se requiere una Máquina Virtual de Java versión 1.5. o superior.

Uso de Applets habilitado

Se requiere tener habilitado el uso de Applets en su navegador.

Certificado digital en formato PKCS12 (PFX)

Para la firma digital de las instrucciones enviadas al INDEVAL, es necesario utilizar un certificado digital en formato PKCS12 el cual tiene la extensión .PFX. La característica de este certificado es que combina un certificado digital (.CER) con una llave privada o clave (.CVE).

La aplicación **InstaladorCertificados** es una aplicación generada por Indeval y es la que debe utilizarse para generar este formato de certificado a partir del certificado digital y llave privada de cada participante.

- La aplicación Instalador de certificados necesita como requisito para poder funcionar tener instalado en la máquina donde se van a generar los certificados .pfx el .Net Framework de Java versión 2.0. el cual puede ser descargado de la página de Microsoft (http://www.microsoft.com/downloads/details.aspx?FamilyID=0856EACB-4362-4B0D-8EDD-AAB15C5E04F5&displaylang=env)

Nota: Para generar el certificado PFX ver Anexo.

Firma Digital

Cada vez que un Participante envíe una instrucción o un conjunto de instrucciones por medio del Portal INDEVAL, deberá firmarlas digitalmente con el certificado digital del participante en formato PFX (Ver la sección Certificado digital en formato PFX). Por lo tanto, esta actividad se repetirá cada vez que el Participante envíe instrucciones por el Portal.

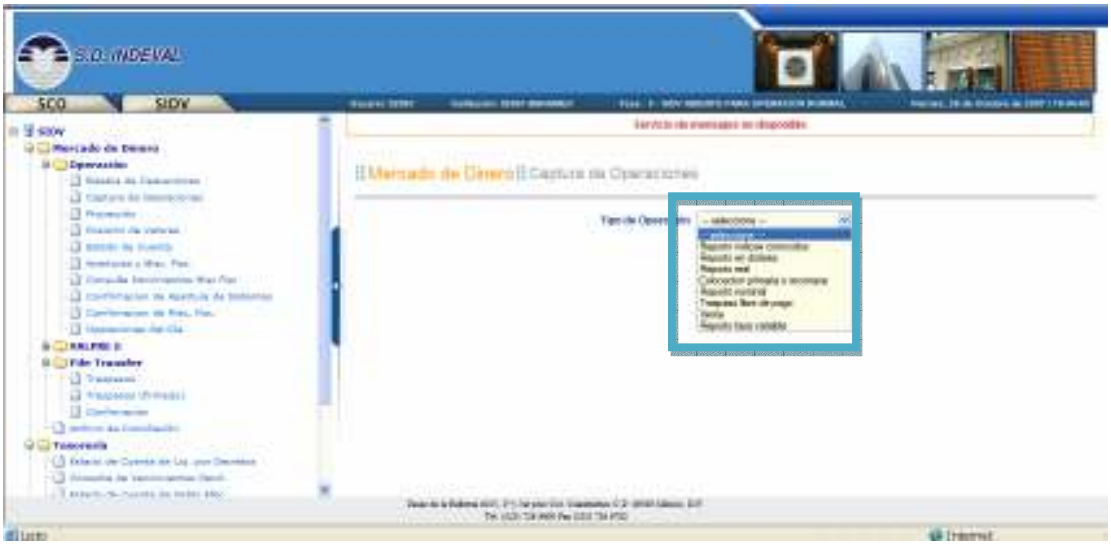
Pasos para el firmado de operaciones

Captura de Instrucciones

Antes de firmar digitalmente una o varias instrucciones, éstas deben ser capturadas en el Portal INDEVAL por medio de un formulario de Captura de Operaciones o por medio del Módulo de File Transfer (En la siguiente sección se describen brevemente estos pasos).

Captura de instrucción individual

1. Ingrese al sistema SD INDEVAL.
2. Seleccione la opción Captura de operaciones.
3. Seleccione el tipo de operación a capturar.



Paso 3. Selección del tipo de Operación.

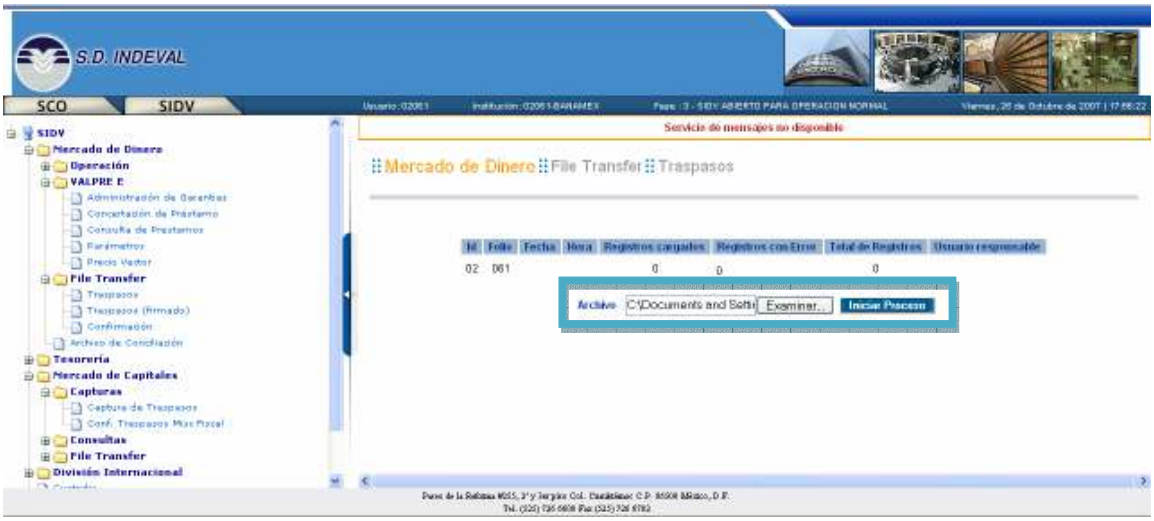
4. Capture la información de la operación a realizar y dé clic en guardar.

Paso 4. Captura de la información y clic en Guardar.

Al terminar la captura de la instrucción, aparecerá la pantalla para la Firma Digital.

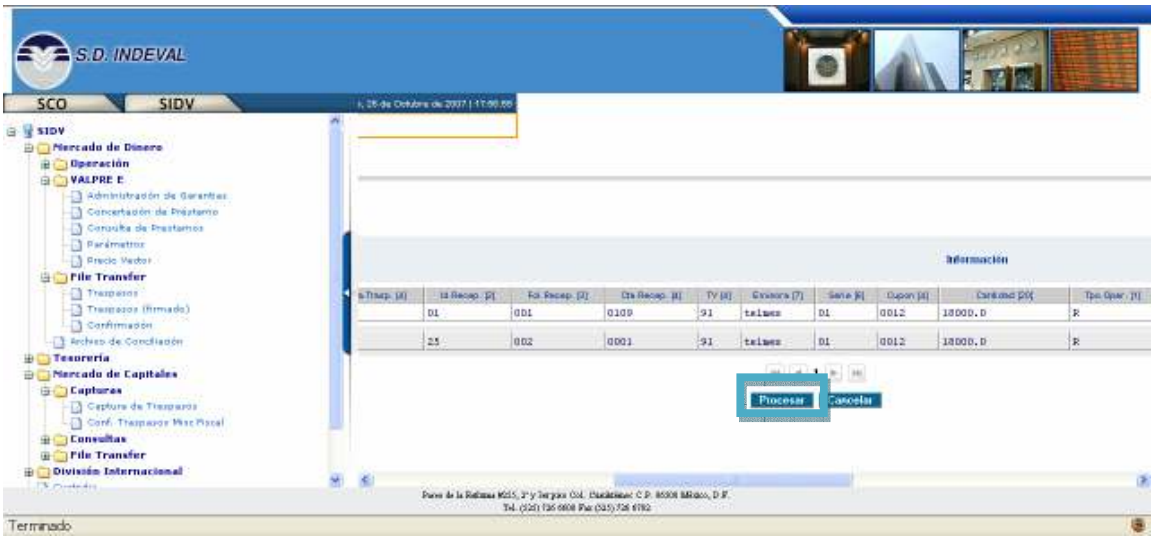
Captura de instrucciones en lote

1. Ingrese al sistema SD INDEVAL
2. Seleccione la opción Traspasos del menú File Transfer.
3. Dé clic en Examinar para seleccionar el archivo que contiene las operaciones que desea realizar.
4. Seleccione el archivo y dé clic en Iniciar Proceso.



Paso 4. Selección de Archivo y clic en Iniciar Proceso

5. El Portal le mostrará el contenido del archivo de operaciones. Seleccione la opción Procesar.



Paso 5. Selección de opción Procesar de instrucciones en lote

Al procesar las instrucciones por lote, aparecerá la pantalla para la Firma Digital.

Firma digital de instrucciones

Al terminar la captura de una instrucción individual, o la carga de un lote de instrucciones por medio del Módulo de File Transfer, si el equipo del Participante cumple con todos los requisitos para la firma digital, aparecerá la pantalla que se carga en el navegador para realizar la firma digital.

A continuación se describen los pasos necesarios para realizar la firma digital de la instrucción o instrucciones capturadas.

1. La pantalla de firma digital aparecerá al finalizar una de las dos siguientes acciones.

    a. El Participante ha dado clic en el botón de **Guardar**, en la pantalla de Captura de operaciones individuales.

    b. El Participante ha dado clic en el botón de **Procesar**, en la pantalla de procesamiento de instrucciones en lote (del Módulo de File Transfer).

2. El Portal desplegará la instrucción o instrucciones a firmar, seguida de un botón para Firmar.

Paso 2. Pantalla de firma digital que despliega la instrucción y el botón Firmar

3. Presione el botón Firmar.

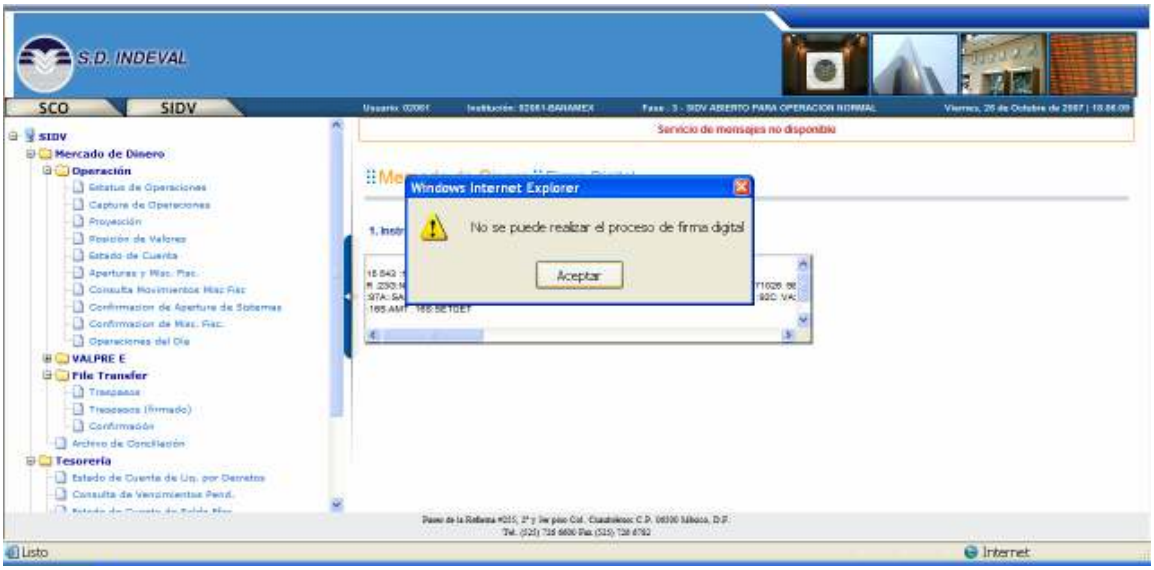
4. El sistema mostrará una pantalla solicitando la contraseña del certificado. Proporcione la contraseña y presione Aceptar.

5. El sistema firma la instrucción o instrucciones y las envía para su procesamiento. El sistema muestra una nueva pantalla indicando el éxito del envio de la operación firmada y su respectivo número de folio de operación.

Paso 5. Pantalla que muestra el mensaje de éxito de la generación de la firma digital de la operación y su folio

Errores en la Firma Digital

Es posible que el Participante no pueda realizar la firma digital de instrucciones por diversas cuestiones técnicas. La siguiente pantalla se mostrará al usuario en caso de que no cumpla con los requisitos para utilizar el mecanismo de Firma Digital.



Pantalla de error en caso de que no se pueda realizar la firma digital.

A continuación se listan los escenarios en que no se podrá usar la firma digital.

1. El usuario cuenta con un navegador Internet Explorer versión menor a 6.0, o un navegador Firefox versión menor a 1.6.

2. El usuario de Internet Explorer tiene deshabilitado el uso de Applets.

3. El usuario de Internet Explorer no tiene una Máquina Virtual de Java (JVM) o es menor a la versión 1.5, y rechaza tanto la instalación de una nueva.

4. El usuario de Firefox intenta firmar múltiples instrucciones (por medio de File Transfer) y tiene deshabilitado el uso de Applets.

5. El usuario de Firefox intenta firmar múltiples instrucciones (por medio de File Transfer), no tiene una Máquina Virtual de Java (JVM) o es menor a la versión 1.5, y rechaza la instalación de una nueva JVM.

Nota: Para validar y corregir los prerrequisitos necesarios para realizar la firma digital, ver la sección de Prerrequisitos.

Las recomendaciones para resolver estos problemas son los siguientes:

a. Instalar la máquina virtual de Java (JVM) 1.5.

b. Habilitar el uso de Applets en el navegador.

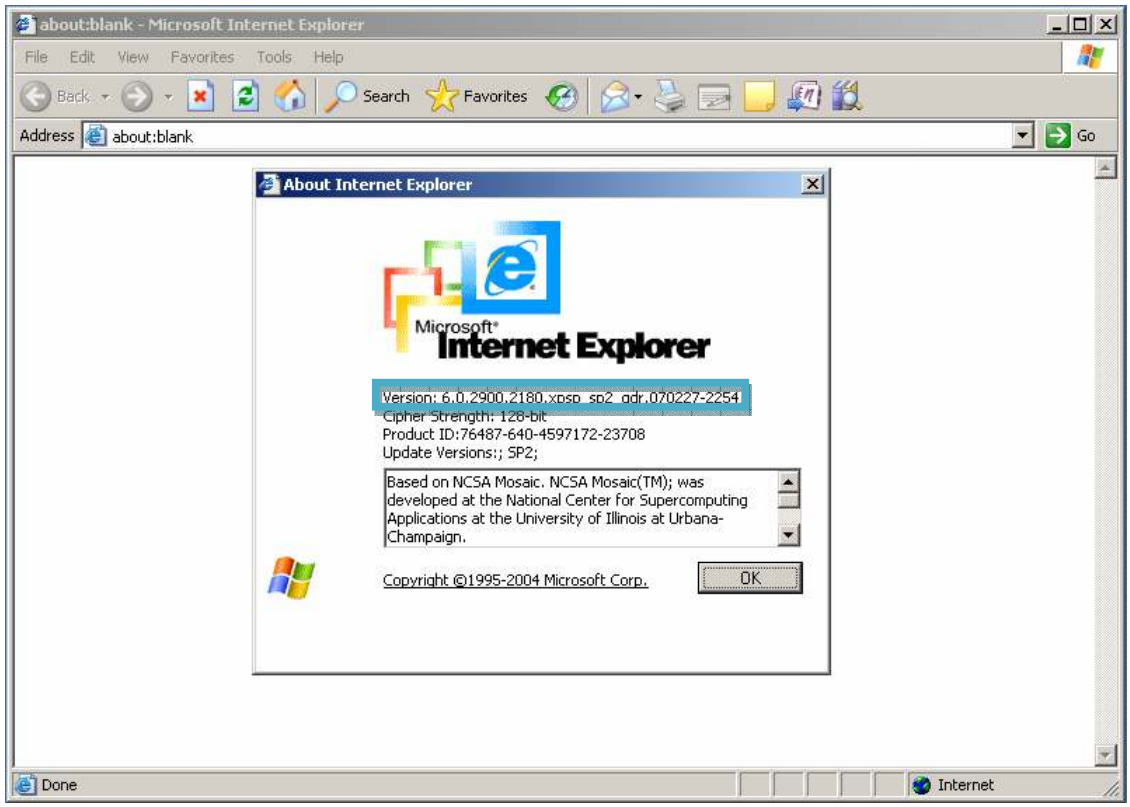
Anexos

Validación de versión del navegador de internet

Para conocer la versión de su navegador siga los siguientes pasos.

Para Internet Explorer

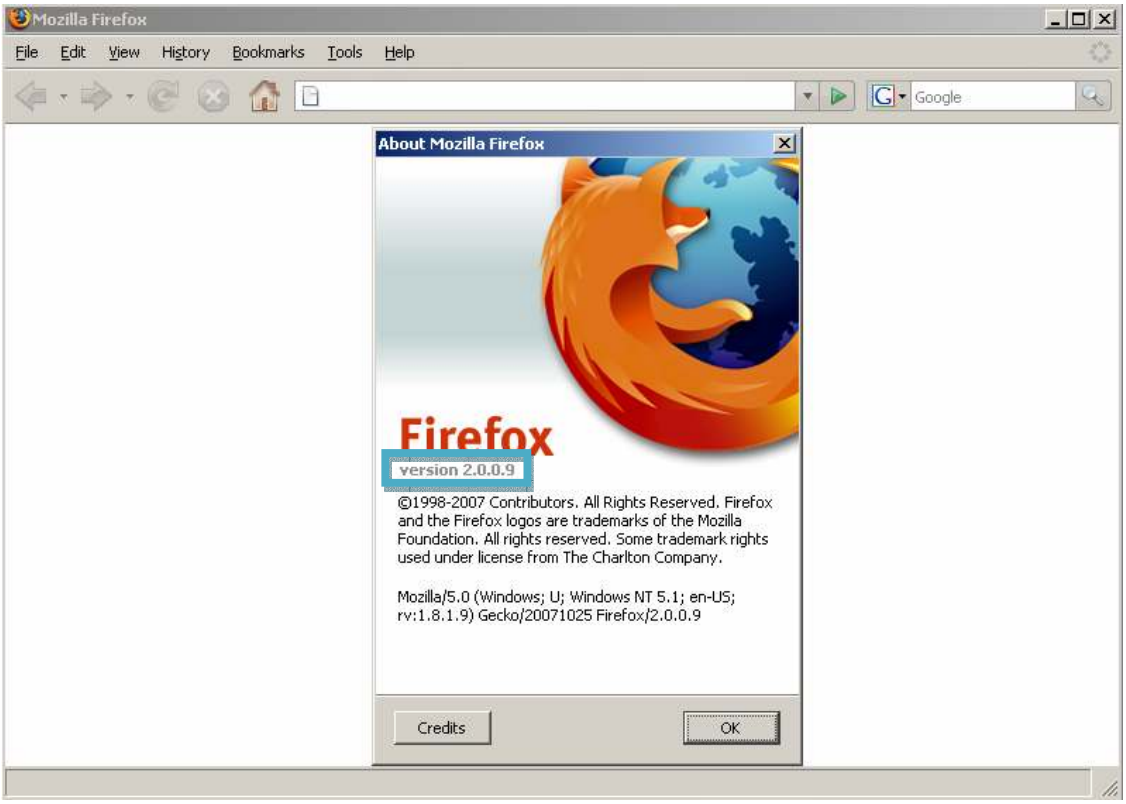
1. Seleccione el menú **Ayuda**.
2. Seleccione la opción **Acerca de Internet Explorer**.
3. Verifique que la Versión sea igual o superior a 6.0.



Paso 1. Validación de versión en Internet Explorer.

Para Firefox

1. Seleccione el menú **Ayuda**.
2. Seleccione la opción **Acerca de Mozilla Firefox**.
3. Verifique que la Versión sea igual o superior a 1.6.


Mozilla Firefox
File Edit View History Bookmarks Tools Help
Google
About Mozilla Firefox
Firefox
version 2.0.0.9
©1998-2007 Contributors. All Rights Reserved. Firefox and the Firefox logos are trademarks of the Mozilla Foundation. All rights reserved. Some trademark rights used under license from The Charlton Company.
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.9) Gecko/20071025 Firefox/2.0.0.9
Credits
OK

Paso 2. Validación de versión en Firefox.

Instalación de Navegador de Internet

Si no cuenta con una versión igual o superior a 6.0 para Internet Explorer, o 1.6 para Firefox, puede instalar la última versión del navegador que desee siguiendo los siguientes pasos.

1. Acceda al sitio web del navegador que desea instalar. Ver la página Referencias.
2. Descargue el archivo de instalación a su disco duro.
3. Dé doble clic en el archivo de instalación y siga las instrucciones del instalador para instalar el navegador.

Validación de JVM

La manera más sencilla de validar la versión de la Máquina Virtual de Java que esta instalada es acceder la página de Verificación de Instalación de Java. Ver la página Referencias.

1. Por medio de su navegador, acceda a la página de Verificación de Instalación de Java.

2. Verifique que el valor de Java Runtime Version sea igual o mayor a 1.5.

Address
vendor=Sun+Microsystems+Inc.&os=Windows+XP&os_version=5.1
Duke's Zone | Games | Mobile | Desktop | Java
JAVA SOFTWARE for Your Computer
VERIFY YOUR JAVA SOFTWARE INSTALLATION
WE DETECTED YOUR JAVA ENVIRONMENT AS FOLLOWS:
Description
Your Environment
Java Runtime Version
1.5.0_06
CONGRATULATIONS, you have the Latest version of Java!

Instalación de JVM

Si no cuenta con una versión igual o superior a 1.5 de la Máquina Virtual de Java, acceda a la página de descargas de Java.

1. Acceda al sitio web de Java. Ver la página Referencias.

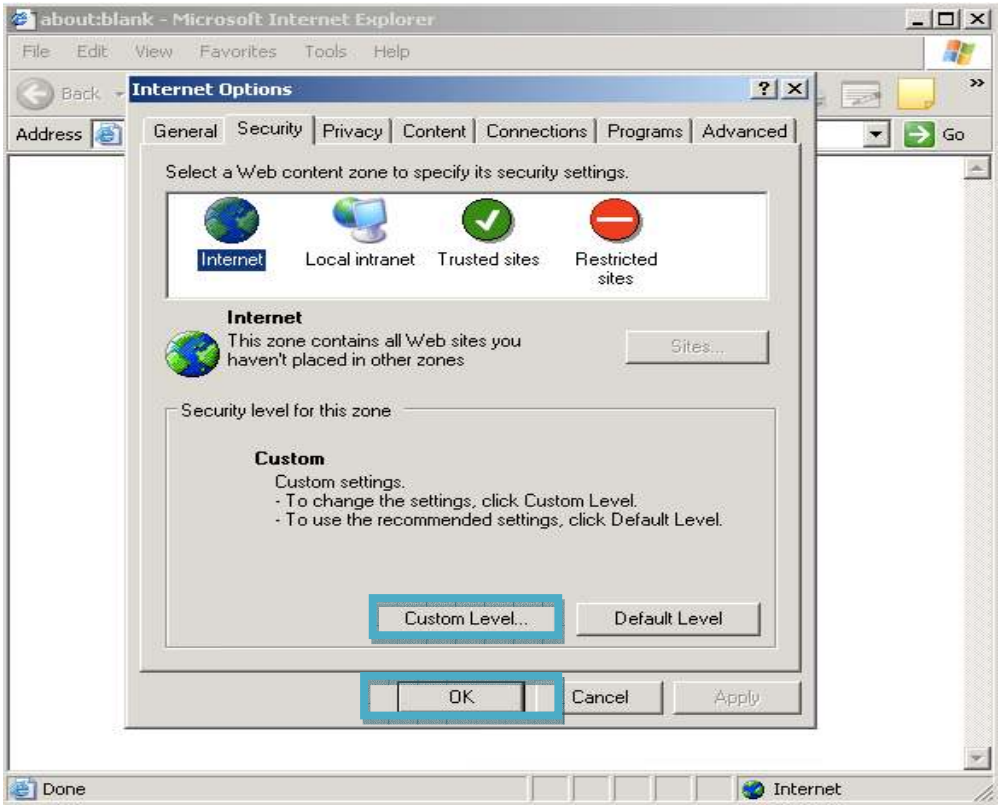
2. Descargue el archivo de instalación a su disco duro.

3. Dé doble clic en el archivo de instalación y siga las instrucciones del instalador para instalar la versión de Java deseada.

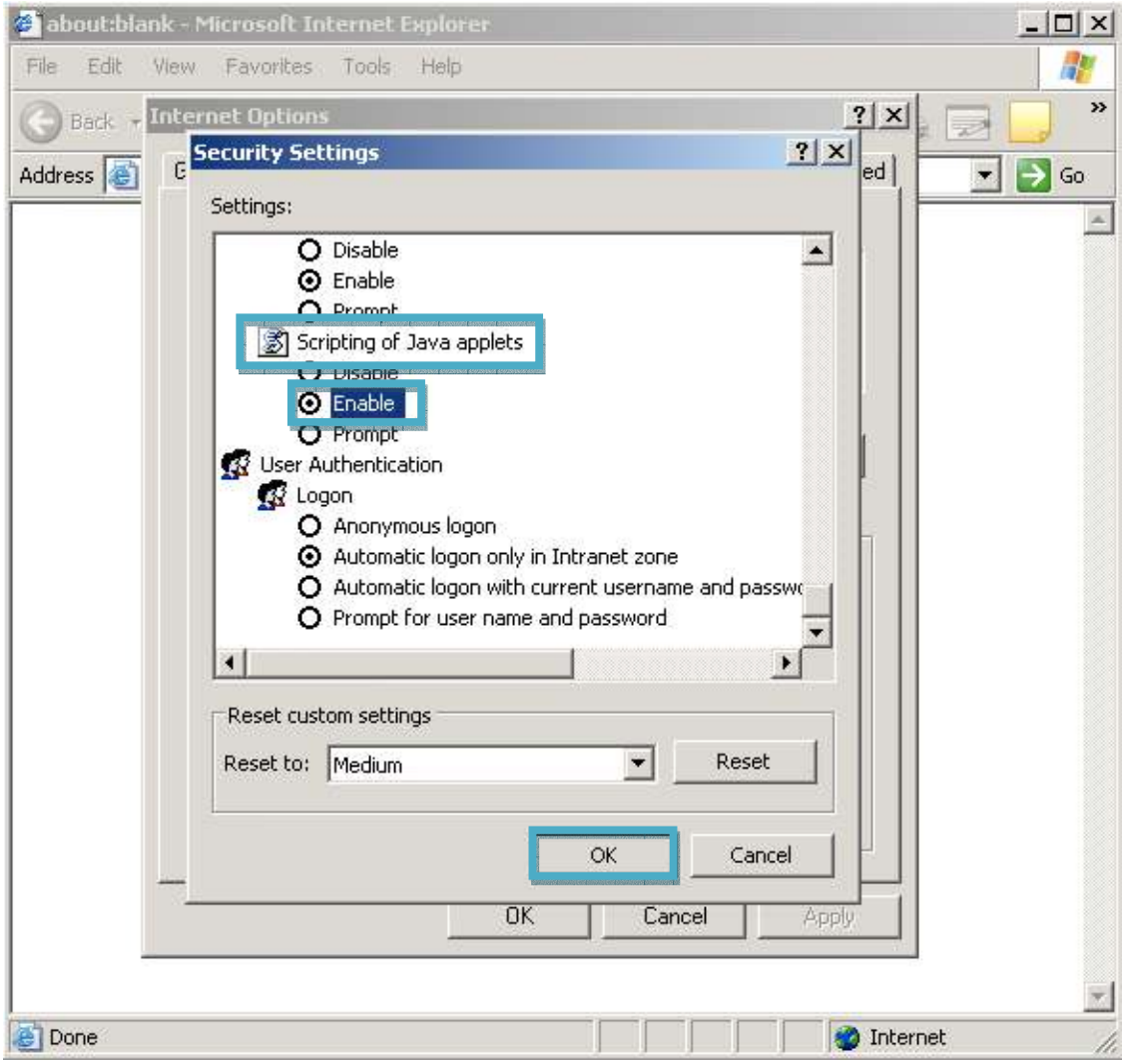
Verificación de habilitación de Applets para Internet Explorer

Para validar si cuenta con Applets habilitados en Internet Explorer, siga los siguientes pasos:

1. Seleccione el menú **Herramientas**.
2. Seleccione el submenú **Opciones de Internet**.
3. Seleccione la pestaña de **Seguridad**.
4. Seleccione la zona de **Internet**, y dé clic en **Niveles Personalizados** (Custom Levels).



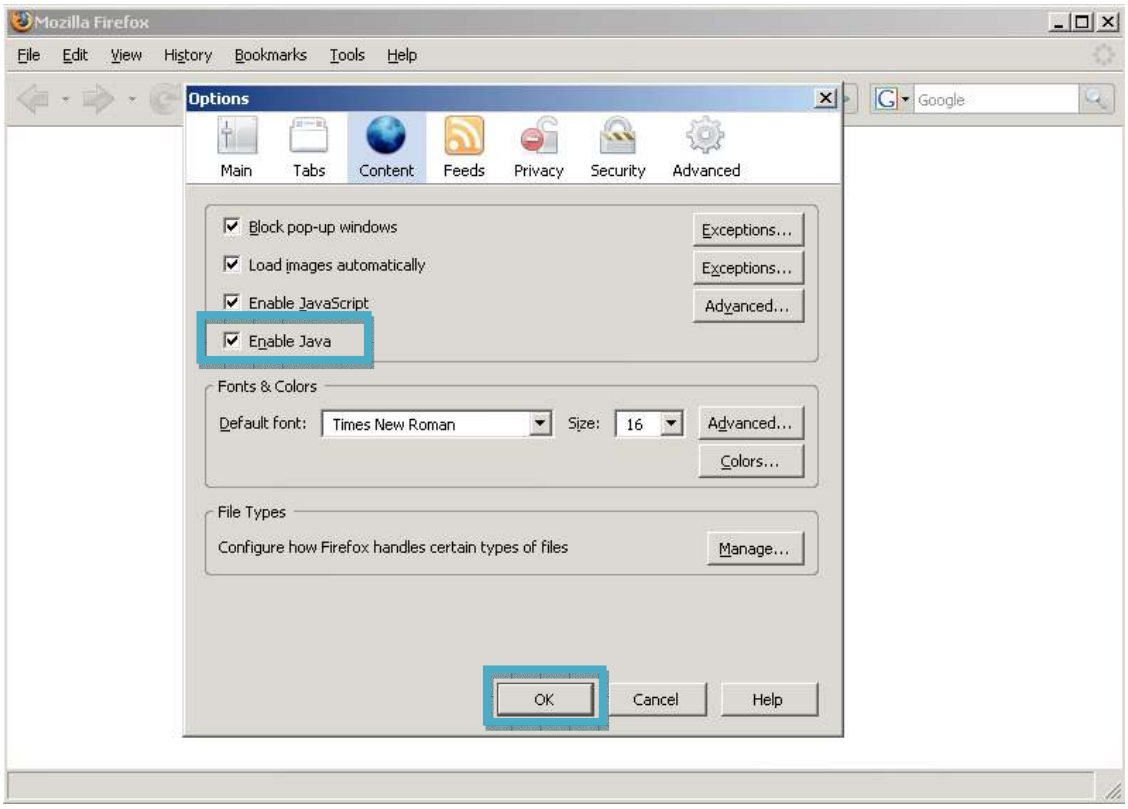
6. Busque la opción de **Ejecución de Applets Java** (Scripting of Java Applets) y verifique que esté en la opción **Habilitado** (Enable).



Verificación de habilitación de Applets Para Firefox

Para validar si cuenta con Applets habilitados en Firefox, siga los siguientes pasos:

1. Seleccione el menú **Herramientas**.
2. Seleccione el submenú **Opciones**.
3. Seleccione la pestaña de **Contenido**.
4. Verifique que se encuentra activada la casilla **Habilitar Java** (Enable Java).



Paso 6. Verificar que está seleccionada la casilla de Habilitar Java

Habilitar uso de Applets en Internet Explorer

Vuelva al paso de **Verificación Para Internet Explorer**.

Si en el paso 6 de la Verificación detecta que está Deshabilitado (**Disable**) el uso de Applets Java, es necesario habilitarlos. Siga los mismos pasos descritos en la sección anterior hasta llegar a las **Opciones de Seguridad**, y seleccione **Habilitar** (Enable) la **Ejecución de Applets Java** y presione el botón de **Aceptar** (OK). Repita estos pasos para tres zonas de seguridad: **Internet**, **Intranet Local** y **Sitios Seguros**.

Habilitar uso de Applets en Firefox

Vuelva al paso de **Verificación Para Firefox**.

Si en el paso 4 de la Verificación detecta que no está seleccionada la casilla de Habilitar Java (Enable Java), es necesario habilitarla. Siga los mismos pasos descritos en la sección anterior hasta llegar a **Opciones**, y seleccione **Habilitar Java** (Enable Java) y presione el botón de **Aceptar** (OK).

Generación de Certificados PKCS12

El Participante debe contar con los siguientes elementos para realizar esta actividad:

1. La aplicación **Instalador de Certificados** (InstaladorCertificados.exe).
2. Un archivo con un certificado digital (.cer,crt) obtenido de una entidad Certificadora.
3. Un archivo con una llave privada (.cve) obtenida obtenido de una entidad Certificadora.
4. La contraseña de la llave privada.

Adicionalmente, el Participante deberá proveer:

1. Una contraseña (nueva) para proteger el nuevo certificado en formato PFX.
2. La ruta en el sistema de archivos (disco duro) donde desea que se almacene el nuevo certificado.

5.1.4.2 Pasos para generar el Certificado PKCS12

Para generar un certificado digital en formato PFX, el Participante debe realizar los siguientes pasos:

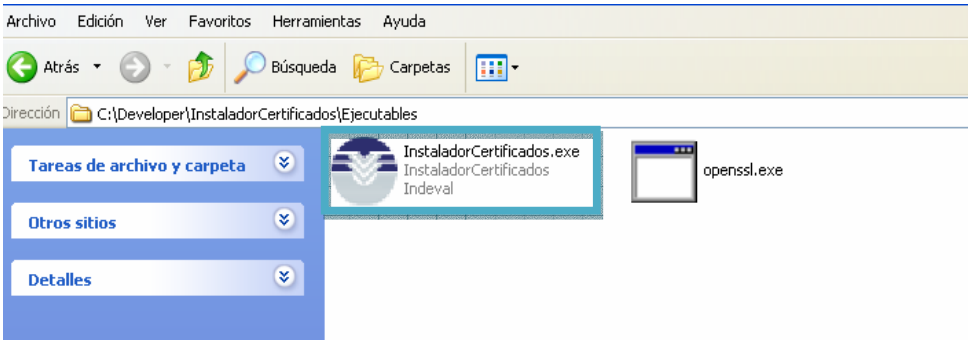
1. Ejecutar la aplicación InstaladorCertificados.exe
2. Proporcionar la información necesaria para generar el nuevo certificado PFX (certificado digital, llave privada y contraseña, nueva contraseña para el certificado a generar, y ruta donde se almacenará).

En la siguiente sección, se explicarán de manera detallada y gráfica cada una de estas actividades.

Instrucciones

1. Ejecutar la aplicación InstaladorCertificados.exe

1.1 Localice en el sistema de archivos el ejecutable InstaladorCertificados.exe. Note que hay un archivo adicional llamado openssl.exe. Este archivo tiene funcionalidad requerida por el Asistente de Instalación de Certificados (InstaladorCertificados.exe), por lo que no debe ser eliminado o movido por ninguna razón.



Paso 1.2. Icono del ejecutable de InstaladorCertificados.exe

1.2 Dé doble clic sobre el icono de InstaladorCertificados.exe, o seleccione el icono y dé Enter.

1.3 El sistema mostrará una pantalla de captura de información.

Generador de Certificado PFX
Indicaciones Generales:
Para la instalación del certificado PFX se requieren los siguientes pasos:
1. Combinar el certificado (.cer) y su llave (.cve)
Mediante esta herramienta ud. podrá generar su propio archivo PFX a partir de su contraseña (.cve) y su certificado expedido por la autoridad certificadora (.cer)
Datos de Captura
a) Seleccione Certificado (.CER / .CRT)
b) Seleccione Llave (.CVE)
c) Escriba Contraseña Clave (.CVE)
d) Escriba Contraseña Certificado PFX
e) Confirme Contraseña Certificado PFX
Generar Certificado PFX

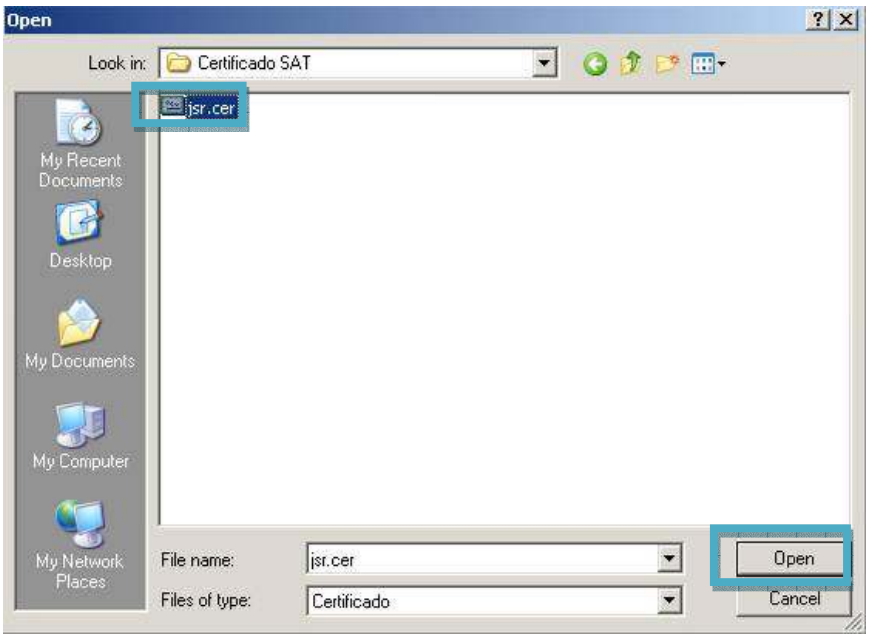
Paso 1.3. Pantalla principal del Instalador de Certificados

2. Datos de Captura.

2.1 Dé clic en el botón **a) Seleccionar Certificado (.CER,CRT)**.

2.2 El sistema le mostrará una pantalla que le permitirá navegar en su sistema de archivos (disco duro).

2.3 Seleccione el archivo que corresponde a su certificado digital. El archivo debe tener la extensión **.CER o CRT**. Dé Enter, o presione el botón Open (Abrir).

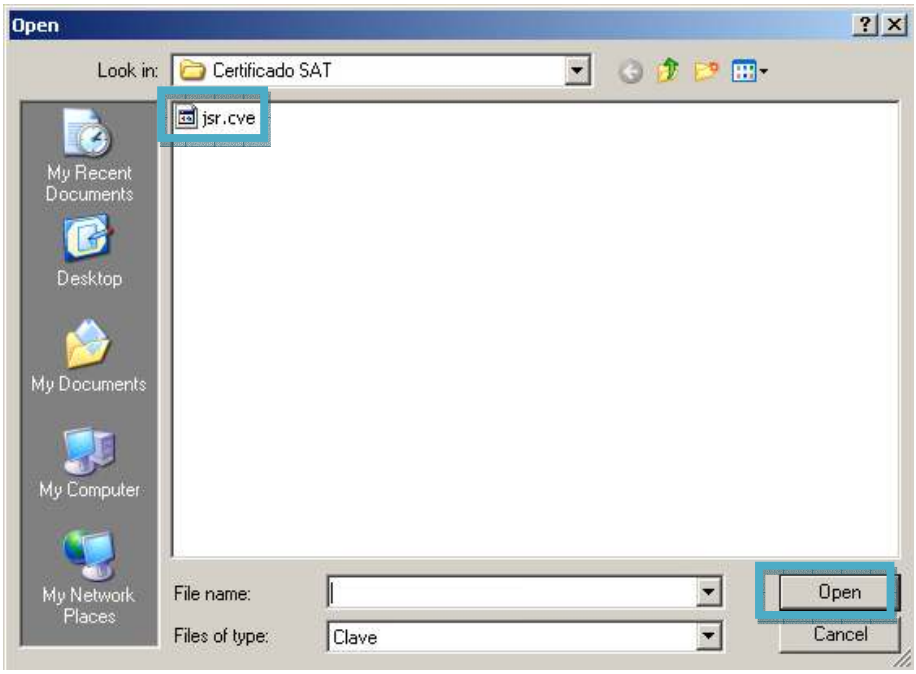


Paso 2.3 Selección del certificado digital (.CER,CRT)

2.4 Dé clic en el botón **b) Seleccionar Clave (.CVE)**.

2.5 El sistema le mostrará una pantalla que le permitirá navegar en su sistema de archivos (disco duro).

2.6 Seleccione el archivo que corresponde a su llave privada, obtenida de una autoridad certificadora. El archivo debe tener la extensión **.CVE.** Dé Enter, o presione el botón Open (Abrir).



Paso 2.6 Selección de la llave privada (.CVE)

2.7 Capture la contraseña (o *passphrase*) de la llave privada.

2.8 Capture una nueva contraseña para el certificado PFX.

2.9 Capture nuevamente la nueva contraseña para el certificado PFX (confirmación).

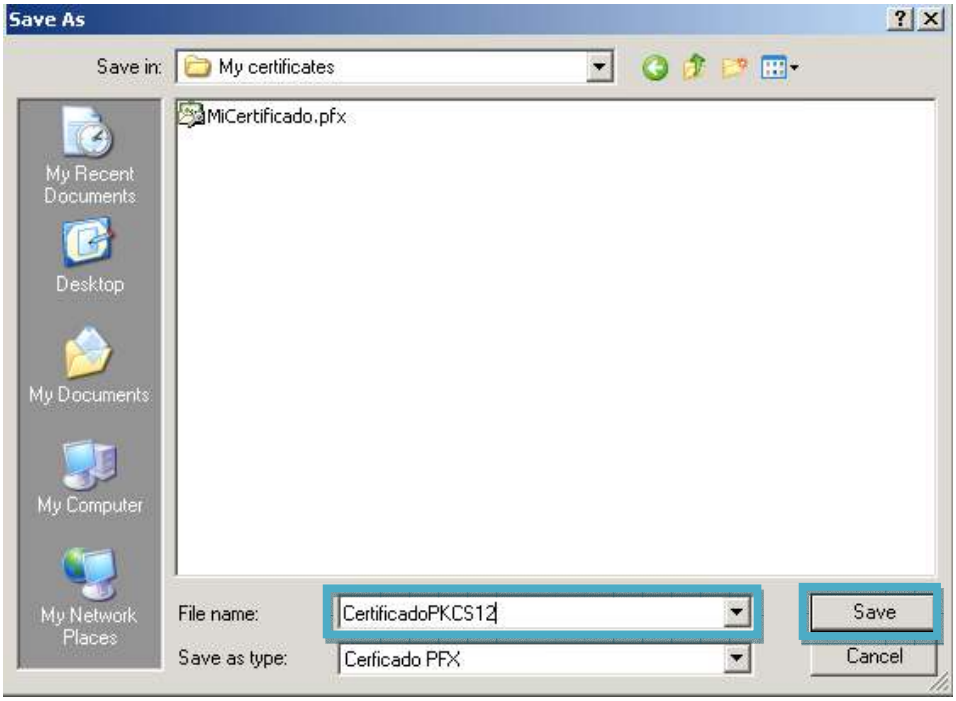
2.10 Dé clic en el botón Generar e Instalar Archivo Certificado PFX.

Generador de Certificado PFX
Indicaciones Generales:
Para la instalación del certificado PFX se requieren los siguientes pasos:
1. Combinar el certificado (.cer) y su llave (.cve)
Mediante esta herramienta ud. podrá generar su propio archivo PFX a partir de su contraseña (.cve) y su certificado expedido por la autoridad certificadora (.cer)
Datos de Captura
a) Seleccione Certificado (.CER / .CRT)
C:\java\certificados\pruebas cross
b) Selecciona Llave (.CVE)
C:\java\certificados\pruebas cross
c) Escriba Contraseña Clave (.CVE)
d) Escriba Contraseña Certificado PFX
e) Confirme Contraseña Certificado PFX
Generar Certificado PFX

Paso 2.10 Pantalla lista para Generar un Certificado PFX

2.11 El sistema le mostrará una pantalla que le permitirá navegar en su sistema de archivos (disco duro).

2.12 Seleccione un folder en su sistema de archivos para almacenar el certificado (por ejemplo: Mis documentos/Mis certificados) y capture un nombre para el certificado (por ejemplo: MiCertificado). Presione Save (Guardar) o dé Enter.



Paso 2.12 Pantalla de selección de ruta de guardado del certificado

Nota importante: Es importante que recuerde la ruta donde guarda su certificado PFX, pues deberá localizar el certificado cada vez que firme digitalmente una o varias instrucciones en el Portal INDEVAL. Si lo desea, puede crear una nueva carpeta llamada Mis Certificados dentro de su carpeta Mis documentos. Con esto se tiene instalado el certificado digital dentro de su equipo.

Recomendaciones

Respaldo de Certificado Digital y Llave Privada

Como una medida de seguridad y con la finalidad de volver a generar el certificado PFX de nuevo en caso de que este haya sido eliminado del sistema de archivos del equipo, es recomendable tener un respaldo seguro del certificado digital y llave privada. La falta de uno de los dos provocaría que no se pudiera generar su certificado PFX de nuevo, en caso de que sea necesario volver a generarlo.

Generación de Certificados PFX

Al generar su certificado pfx, verifique que el par de llave privada y certificado que va a utilizar tengan el mismo formato (PEM para texto o DER para binarios), ya que de lo contrario obtendrá un error al generarlos.

Formato	Tipo	Codificación	Extensión
DER	Llave privada	Binario	.key
DER	Certificado	Binario	.cer
PEM	Llave privada	Texto	.cve
PEM	Certificado	Texto	.crt

Verifique que el tipo de certificado y llave privada a utilizar de acuerdo a su extensión corresponde a archivos binarios o de texto.

Ver apartado de certificados para mayor detalle.

Rutas de almacenamiento para los certificados

Para mayor facilidad de localizar sus certificados PFX dentro de su equipo es recomendable crear una carpeta en una ubicación fácil de encontrar y recordar, como puede ser Mis Documentos y bajo esta crear una carpeta que tenga un nombre relacionado con los certificados PFX.

Un ejemplo puede ser: C:\Documents and Settings\usuario\Mis Documentos\certificadosPFX.

Uso de contraseñas seguras para los certificados PFX

Todos los usuarios deben saber que como medida de seguridad, no se deben compartir certificados y contraseñas de llaves privadas y certificados PFX, esto con la finalidad de que otros usuarios no hagan un mal uso de esta información que es de alta confidencialidad.

Cuando se genere la contraseña de su certificado PFX, se recomienda que esta se componga de la siguiente manera: caracteres alfabéticos, numéricos, caracteres especiales (. #@ $, etc.) y con una longitud igual o mayor a 8 dígitos. No usar como contraseña, fecha de cumpleaños, secuencia numérica del 1 al 8, nombre de hijos etc.

Esto debido a que compañeros de trabajo puedan conocer esa información y con ella hacer un uso indebido para firmar con sus certificados.

Contraseñas no sugeridas

Nombres de personas (Juan Hernandez)

Fechas de cumple años (12-dic-2001)

Mexico DF.

Utilice contraseñas que le signifiquen algo a usted y que presente un reto el memorizarla si alguien la visualiza, por ejemplo:

Jh!32_df1985

Esta contraseña podría presentar algún problema para recordarla si no se sabe exactamente lo que puede significar:

Jh.- Juan Hernandez

32.- Edad actual

df.- Ciudad donde vive

1985.- Fecha de un acontecimiento importante.

!_ .- Caracteres de separación.

Todos estos elementos nos podrían proporcionar una contraseña segura con elementos fáciles de memorizar, pruebe generar una contraseña que contenga dos o tres elementos fáciles de recordar para usted, así como jugar con las letras que lo componen (usar mayúsculas y minúsculas), y ademas cambiar los caracteres de separación.

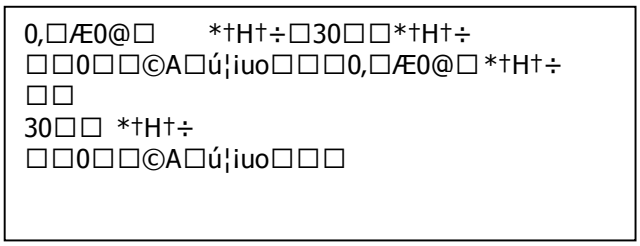
Información sobre certificados Digitales

En criptografía, X.509 es un estándar UIT-T para infraestructuras de claves públicas (en inglés, Public Key Infrastructure o PKI).

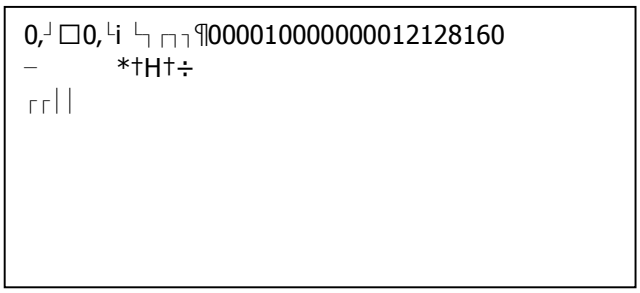
X.509 es la pieza central de la infraestructura de clave pública y es la estructura de datos que enlaza la clave pública con los datos que permiten identificar al titular. Su sintaxis se define empleando el lenguaje ASN.1 (Abstract Syntax Notation One) y los formatos de codificación más comunes son:

- **DER** (Distinguished Encoding Rules).- Este tipo de archivos están codificados en formato binario y las extensiones mas comunes para las llaves privadas son .***key*** y para los certificados .***cer***.

  Si se abre un archivo binario en un editor de texto, cada grupo de ocho bits serán traducidos normalmente como un caracter aislado y seguramente se observará una secuencia de datos complicada y casi sin sentido, ininteligible de caracteres.



Ejemplo de certificado en formato DER



Ejemplo de llave privada en formato DER

- **PEM** (Privacy-enhanced Electronic).- Este tipo de archivos están codificados en formato de texto y las extensiones mas comunes para almacenar los certificados son ***.crt*** para los certificados y ***.cve*** para las llaves privadas.

-----BEGIN CERTIFICATE-----

MIIDTjCCAregAwIBAgIUMDAwMDAxMDAwMDAxMDAwMDkxOTEwDQYJKoZIhvcNAQEF
BQAwggFGMQswCQYDVQQGEwJNWDEVMBMGA1UECBMMTWV4aWNvLCBELkYuMRkwFwYD
VQQHExBDaXVkYWQgZGUgTWV4aWNvMRgwFgYDVQQKEw9CYW5jbyBkZSBNZXhpY28x
JDAiBgNVBAsTG0luZnJhZXN0cnVjdHVyYSBJbmZvcm1hdGljYTEpMCcGA1UEAxMg
QWdlbmNpYSBDZXJ0aWZpY2Fkb3JhIGRlIHBydWViYXMxFjAUBgNVBC0TDS1TSU4t
UkVHSVNUUk8xFjAUBgNVBAwTDUFDIGRlIHBydWViYXMxETAPBgZ1iF2PNRETBTA2
MDU5MS8wLQYGdYhdjzUTEyNBdi4gQ2luY28gZGUgbWF5byBOby4gNiBDb2wuIENl
bnRybzEmMCQGCSqGSIb3DQEJARYXYWVkZWxlb25AYmFueGljby5vcmcubXgwHhcN
MDYwNjIxMTk0NjE4WhcNMDgwNjIxMTk0NjE4WjB/MQswCQYDVQQGEwJNWDEZMBcG
A1UECBMQRGlzdHJpdG8gRmVkZXJhbDEZMBcGA1UEBxMQQ2l1ZGFkIGRlIE1leGlj
bzElMCMGA1UEAxMcSmVzdXMgU2FsdmFkb3IgUmFtb3MgQ2FyZG9uYTETMBEGA1UE
LRMKUkFDSjc5MDcyMzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAz1rqBKq3
pH/LMTGBT5L2AfjRqHHQKmcjFhj8++07ztSHxBNddt4VbJf81wcLnBNusZ6N3Bwj
N48nwbwFOcLCxWc/ZGKjYdFALXI1Maf5XzdMyYIksSnvun7tja+aLA7RJYsPek5X
hjf5iuOeep8zvrKIo9NMRYbS4I7tzONhBkcCAwEAATANBgkqhkiG9w0BAQUFAAOB
gQCAMpc0AzloKGP2wNDUpHyROI3vcGNQt4iyF6LvsKbisrJ2Lgqbty0+1/Rsdgas
ZHAniWZrC9KaTYtVG1hgyfv3AOviF+oxAPMoB8y5Jcmn0i1YC0Dar9ToBI6lfEDj
L+8VzcuqwHb7P9JEbQ2lW1W93gb+K5BtLA458JT+/2JGBw==

-----END CERTIFICATE-----

Ejemplo de certificado en formato PEM

-----BEGIN RSA PRIVATE KEY-----

Proc-Type: 4,ENCRYPTED

DEK-Info: DES-EDE3-CBC,5463BC65C5F639FA

/gi4EqK44lUbY0xzhJ21EjIQmkJx9AdFk9qjRRsU500uchEAwFrjJ29VE1wdiAMI
91sL0ZwZsyKxHUBSusVisYx5YfCBZ7tBHgjHiTLl33WclChJJ8ykVVORidcQ6e8x
TwNB0kHbbU1rZ9OqHat1HSfwh6JPfyFMJA2U2txvrcjPSAu/4nrCQy9LXJRII0x+
zFetF9wn7fTFo6DmPLIvFAUIIX6d3ZDhG3txfxEwcotlYLQztqpmi3N6fq8h06dz
TcFIdf7gF+NfQHy0vg11tgLmuzsa9628/0k3sTaF7/l/33glcPQcQFhoXCFgUDH4
8AfbEgRCJL91J+UUvPwziGd/s75VSpz+4UNWXe6fCTThGFQcp/FVInGhLhQYpmiU
RkqAL0UYkAsLQ2M9e1wCx2QD/oG6WEv8SPRHNgmIRck9bNghJ3GVeXUdcexW5BK0
MFaY3iz67lLe0e3z5sj00CcftZMNFx9BdCVnJaiIGGk+oxXd6e+G242jP4XhS5Ah
97ckglzYncoWXDDMFRCszrh+g0GG2z5cY8JM4yP/kxIo4hTBde4dn+a+FOp9s4Q3
YHo5Om7O6T0i1yfmPhZEYxs6B1K9FSjLHD5vNok2VlEk1wXBXAMcSwVCysFDyq4V
ubrUVrWRUwDxecaAAg6fU7yTap0Hh64g6x37kpcDRi+KsU6UOK4FOdkJmU8Vy3vx
Kf9WdfYGkL7Szs8Vysuskvx5M7O/QyZVTINR/m0OxM33av/41TSvnO4BkHKKrdgd
y6L6FsmghSmAoOGE1rImvoYexSB3wyPrHTACa5552dCD6UXJzXRmRQ==

-----END RSA PRIVATE KEY-----

Ejemplo de llave privada en formato PEM

Referencias

Página oficial de Mozilla Firefox. Página para la descarga del instalador del navegador Mozilla Firefox. http://www.mozilla.com/firefox/

Página oficial de Internet Explorer. Página para la descarga del instalador del navegador Windows Internet Explorer. http://www.microsoft.com/windows/downloads/ie/getitnow.mspx

Página de Verificación de Instalación de JVM. Página que permite confirmar la versión de la Máquina Virtual de Java que está instalada en el equipo de cómputo del participante. http://www.java.com/en/download/installed.jsp

Página de descarga de Java. Página que permite descargar el instalador de Java (para actualizar la Máquina Virtual de Java). http://www.java.com/en/download/manual.jsp